Protecting Your Privacy

Keeping an Eye on Your Private

E-mail, the Internet, automated teller machines (ATM), computer banking, long distance carriers and even credit cards make our lives more efficient. However, as our lives become more integrated with technology, keeping our private information confidential becomes more difficult. Electronic transactions can leave you vulnerable to fraud and other crimes. Following a few simple tips can help keep your code from being cracked.

A Word About Passwords

Whether you are on the Internet or an online banking program, you are often required to use a password. The worst passwords to use are the ones that come to mind first – names (yours or those of your friends, relatives, or pets), your street address, etc. The best passwords mix numbers with upper and lowercase letters. A password that is not found in the dictionary is even better. There are programs that will try every word in the dictionary in an effort to crack your security.

Don't be a "Joe" — someone who uses his name as a password.

The weakest link in a security system is the human element. The fewer people who have access to your codes and passwords, the safer your privacy. Avoid breaks in your security by:

- Changing your password regularly.
- Memorizing your password. If you have several, set up a system for remembering them. If you do write down the password, keep it at home or hidden at work. Don't write your password on a post-it note and stick it on your monitor or desk.
- Setting up a special account, or setting aside a different computer, for temporary help and other unauthorized users.
- If you have the option of letting your computer or a Web site remember a password for you, don't use it. Anyone who uses your machine will have automatic access to information that is password protected.

***Never send confidential, financial or personal information via* E-mail**

Shopping in Cyberspace

Ordering merchandise from the Internet is a trend of the future. You can prevent problems before they occur by:

- Doing business with companies you know and trust. If you haven't heard of the company before, research it or ask for a paper catalog before you decide to order electronically. Check with your state consumer protection agency on whether the company is licensed or registered. Fraudulent companies can appear and disappear very quickly in cyberspace.

- Understanding the offer. Look carefully at the products or services the company is offering. Be sure you know what is being sold, the quality being specified, the total price, the delivery date, the return and cancellation policy and all the terms of any guarantee.

- Using a secure browser that will encrypt or scramble purchase information. If there is no encryption software, consider calling the company's 800 number, faxing your order, or paying with a check.

- Never giving a bank account or credit card number or other personal information to anyone you don't know or haven't checked out. Don't provide information that isn't necessary to make a purchase. Even with partial information, con artists can make unauthorized charges or take money from your account. If you have an even choice between using your credit card and mailing cash, check, or money order, use a credit card. You can always dispute fraudulent credit card charges, but you can't get cash back.

Using ATMs, Long Distance Phone Services and Credit Cards

Protect your Personal Identification Number (PIN)

- The PIN is one method used by banks and phone companies to protect your account from unauthorized access. A PIN is a confidential code issued to the cardholder to permit access to that account. Your PIN should be memorized, secured and not given to anyone, not even family members or bank employees. The fewer people who have access to your PIN, the better.

- Never write your PIN on ATM or long distance calling cards. Don't write your PIN on a piece of paper and place it in your wallet. If your wallet and card are lost or stolen, someone will have everything they need to remove funds from your account, make unauthorized debit purchases or run up your long distance phone bill.

Protect Your Privacy and the Privacy of Others

- Be aware of others waiting behind you. Position yourself in front of the ATM keyboard or phone to prevent anyone from observing your PIN. Be courteous while waiting at an ATM or pay phone by keeping a polite distance from the person ahead of you. Allow the current user to finish before approaching the machine or phone.

Protect Your ATM Cards

- An ATM card should be regarded as though it were cash. Avoid providing card and account information to anyone over the telephone.

- When making a cash withdrawal at an ATM, immediately remove the cash as soon as the machine releases it. Put the cash in your pocket and wait until you are in a secure location before counting it. Never use an ATM in an isolated area or where people are loitering.

- Be sure to take your receipt, record transactions and match them against monthly statements. Dishonest people can use your receipt to get your account number. Never leave the receipt at the site.

Protect Your Credit Cards

- Only give your credit card account number to make a purchase or reservation you have initiated. Never give this information over a cellular phone.

- Never give your credit card to someone else to use on your behalf.

- Watch your credit card after giving it to store clerks to protect against extra imprints being made.

- Destroy any carbons. Do not discard carbons, charge slips or receipts that list your credit card number into the trashcan at the purchase counter. Keep these documents in a safe place.

- Protect your purse or wallet, especially when traveling or in crowded situations.

- Save all receipts and compare them to your monthly statement. Report any discrepancies immediately!

- Keep a master list in a secure place at home, with all account numbers and phone numbers for reporting stolen or lost cards.

Lost or Stolen Cards

- Always report lost or stolen cards to the issuing company immediately. This limits any unauthorized use of your card and permits the company to begin the process of issuing a new card.

Crime can be random. But there are steps that limit your chances of becoming a victim. Being aware of the threat of crime — and alert to what you can do to prevent it — will go a long way toward making your electronic transactions safe and private.

Source: National Crime Prevention Council